Information Security and CNS Hardening

Topic: What are the security implications of emerging CNS technologies that need to be considered? How will new aviation security policies impact the design and development of new CNS technologies and related applications?

Marie Stella and Gus Martzaklis, Co-chairs

Kevin Harnett

Crispin Netto

Participants

- Gus Martzaklis (NASA GRC)
- Marie Stella (FAA)
- Kevin Harnett (DoT/Volpe Center)
- Al Homans (ARINC)
- Frank Frisbie (Northrup Grumman IT)
- Bob Stephens (Boeing ATM)
- Ed Rao (DHS/TSA)
- Sethu Rathinam (Rockwell Collins)
- Barry Valentine (GAMA)
- Beth Plentovich (NASA LRC)
- Calvin Ramos (NASA LRC)
- Jon Arneson (Volpe/CSC)
- Mark Freeman (Volpe)
- Doug Rohn (NASA GRC)
- Gary Livack (FAA)
- Don Kauffman (Honeywell * request to be on Av. Sec. CNS WG)
- Crispin Netto (Computer Networks & Software Inc.)

Information Security & CNS Issues

Problem Statement

- Need to articulate the absence of a NAS-wide security policy
- No integrated strategy
- Lack of an Information Security vision
- Need for a policy that includes government, public and private assets
- Lack of funding and commitment
- Security is a concern
  - Globally
  - Commercially
  - General Aviation
  - DoD

Information Security and CNS Hardening

- Recommendations:

  - Consensus on the need for leadership from the FAA

  - Prepare a brief to the Joint Program Office to be presented to the FAA Administrator (Frank, Gus, Marie, Don to provide draft)

    1. To create an entity to establish US policy and compliance on CNS Information Security
    2. Distribute the policy internally among related US organizations
    3. Distribute policy to various industry groups (AEEC, ICAO etc..)
    4. Communicate policy to the international community
    5. Joint Program Office (JPO) could advocate the recommendations to the FAA Administrator.

Unique research/technologies needed for aviation security

1. Traffic surveillance with respect to position, jamming/spoofing
2. Development of secure multicast for aviation environment
3. Need to look at scalability of IPv4, IPv6
4. Mitigation strategies for Info/CNS infrastructure “crashes”
   - Re-routing
   - Dynamic re-allocation of resources
5. Need for a secure database(s) (for e.g., SWIM) and delivery of TFR/Protected Area for situation awareness in real-time
6. Ability to perform analysis of system impact of security technologies/services on CNS infrastructure
7. Model to quantify performance tradeoffs (risk, QoS, Cost)
8. Need for a capability for confidentiality link while maintaining integrity and availability between FD-FD, FD-ATC, Law Enforcement/DoD
9. Need for IP and ATN Firewalls and scanners without degrading operations
10. General approach to leverage COTS technologies & best practices

Unique research/technologies needed for aviation security (cont.)

11. Accept the fact that Information Security breaches will happen. Need tools for Intrusion Detection and Mitigation
    - Detect, isolate & restore
    - Evaluate, correct & test
12. Anti-viral & “fortress” processor for key systems
13. Use of portable & wireless networks on aircraft (Industry beginning to look at it)